KENTUCKY RETIREMENT SYSTEMS
DATA PROTECTION POLICY

Approval Date: August 20, 2008

Statement of the Data Protection Policy:

As outlined by KRS 61.661, Kentucky Retirement Systems (KRS) is responsible for protecting the confidentiality of its members' data. This policy serves to facilitate KRS' compliance with all applicable state and federal laws and regulations regarding data privacy and protection, including the Health Insurance Portability and Accountability Act (HIPAA).

Responsibility for Compliance:

Each division is responsible for assuring that entities within their organizational authority have been made aware of the provisions of this policy, that compliance is expected, and that violation of this policy may result in disciplinary action pursuant to KRS personnel policies up to and including dismissal and/or civil penalties prescribed by state and federal laws.

Exemptions to this policy shall be requested by submitting a completed KRS Security Exemption Request form to the KRS Information Security Officer (ISO).

Purpose:

The purpose of this policy is to establish and implement comprehensive data protection policy and standards governing KRS' secure use, management, sharing, disclosure, transfer, and storage of data.

DATA PROTECTION STANDARDS

Policy: KRS shall protect against the unauthorized or accidental disclosure, misuse, modification or loss of data, whether intentional or accidental, and shall implement the necessary standards and controls to ensure the confidentiality, integrity, and availability of KRS information assets. In addition, KRS shall collect and utilize personally identifiable information and other sensitive data only to the extent that it is needed to fulfill operational or legal requirements.

Section 1: Employee/Contractor Responsibilities

1. KRS employees/contractors shall:

   a. Refrain from any violation of KRS policy and/or any local, state, or federal law governing information privacy and its use.

   b. Refrain from accessing sensitive KRS data unless it is required to accomplish specific job duties assigned as a KRS employee/contractor.

   c. Protect the confidentiality, integrity, and availability of any KRS data to which access has been granted, regardless of the method used to retrieve or display it.

d. Refrain from making any unauthorized modifications to any data that is accessible either through legitimate granted access or incidental access.

e. Adhere to all software licensing agreements and copyrights and refrain from the download, distribution, installation, or use of pirated software or copyrighted materials for which the user has not acquired appropriate authorization/permission to use.

f. Refrain from logging onto or attempting to logon to another employee’s computer using the employee’s userID/password.

g. Refrain from accessing or attempting to access another employee’s files without the permission of the employee unless a KRS Security Exemption Request form has been approved.

.

h. Refrain from attempting to compromise the security of KRS business resources or information assets unless the activity pertains to the legitimate internal assessment/audit of the KRS information infrastructure and is authorized by the KRS Information Security Officer.

i. Ensure the proper disposal of all sensitive data, regardless of its form, in accordance with the KRS Computer Sanitization Policy.

Section 2: Data Classification

1. KRS shall identify all information systems and the data collected, processed and stored by those systems.

2. Each KRS system shall be assigned a business owner that shall serve as the primary operational manager throughout the system’s life cycle. The business system owner shall be the actual business process owner rather than the KRS Division of Information Technology.

3. KRS shall classify all KRS data according to sensitivity level and shall implement the security requirements and controls listed for each of the data classifications. If KRS information is stored by a third party, the third party must contractually abide by these requirements.

4. KRS shall require that all employees and contractors receive initial and ongoing training on this policy and their responsibilities to protect and secure KRS business resources and information assets.

Section 3: Data Collection and Utilization

1. Data shall be obtained for purposes that are lawful and necessary to conduct KRS business and shall not be utilized or maintained in a manner incompatible with those purposes.

2. Data shall be accurate, current, and retained in accordance with internal data retention policies or as established by law or the Kentucky Department for Libraries and Archives (KDLA).

3. KRS shall not collect and/or store Social Security numbers in processes, procedures, or documentation unless it is required by a federal or state agency or a legitimate business need. A unique identifier shall be used for all processes that do not explicitly require a Social Security number.

4. KRS shall require that only the last four digits of a Social Security number be used in electronic mail (email), paper correspondence, reports, or anywhere the use of the full Social Security number is not warranted.

5. Sensitive KRS data shall be encrypted in accordance with the KRS Encryption Policy.

6. Email containing personal identifiers such as the last four digits of Social Security numbers or other sensitive data shall employ strong encryption during transmission in accordance with the KRS Encryption Policy.

7. Passwords, personal identification numbers (PINs), and full Social Security numbers shall be prohibited from being sent via email unless encrypted in accordance with the KRS Encryption Policy.

8. Data shall be copied, printed or duplicated only when necessary and shall be labeled appropriately as outlined in the KRS Data Classification Matrix.

9. All printed materials containing sensitive data must be immediately recovered from printers, copiers, and fax machines.

10. Hard copy documentation containing sensitive data must be securely stored when not in use.

11. Sensitive data shall not be copied to or stored on local workstation drives, mobile electronic devices, home computers, or any device that can be easily stolen or compromised. The KRS ISO shall approve exemptions to this policy.

12. The use of shared network drives to share or exchange sensitive data internally is prohibited unless access rights/permissions have been restricted to authorized individuals only.

Section 4: System Development/Change Management

1. All security requirements for new system development or existing system modification shall be identified during the feasibility phase of the project and shall be documented as part of the overall business case for a KRS information system.

2. Security controls shall be documented at the application level and in KRS security standards, guidelines, and procedures for system development.

3. KRS production data shall not be used for development and/or testing purposes unless sensitive data elements are replaced with random, scrambled, or concatenated data prior to use. The test data shall be protected and controlled during its lifecycle.

4. All application input data shall be validated to detect data input errors. The checks performed on the client side shall also be performed at the server to ensure data integrity.

5. Application design shall ensure that controls are implemented to minimize the risk of processing failures leading to a loss or corruption of data.

6. KRS shall require the separation of the system development, test and production environments either logically or physically. Processes must be documented and implemented to govern the transfer of software from the development environment to the production platform. The following controls shall be considered:

   a. Development software and tools shall be maintained on computer systems isolated from the production environment, either by housing on physically separate computers or by access-controlled domains or directories.

   b. Access to compilers, editors and other system utilities shall be removed from production systems when not required.

   c. Logon procedures and environmental identification shall be unique for production testing and development.

   d. Controls shall be in place to issue short-term access to development staff to correct problems with production systems allowing only necessary access.

7. A formal change management process shall be developed, documented, and utilized for all changes to the KRS computing environment.

Section 5: Data Management

1. Access to KRS business systems and data shall be provided in accordance with the KRS Access Control Policy.

2. Data shall be stored on KRS business resources only and encrypted in accordance with the KRS Encryption Policy.

3. Separation of duties shall be implemented where practical to reduce the risk of accidental or deliberate system misuse. Whenever the separation of duties is impractical, other compensatory controls such as the monitoring of activities, audit trails and management supervision shall be implemented and segregated from the security function.

4. KRS shall develop and implement comprehensive business continuity/disaster recovery plans as outlined in the KRS Business Continuity/Disaster Recovery Planning Policy to protect KRS assets in the event of an interruption of service.

5. All KRS data, applications, system configuration files and other mission critical data or software shall be backed up to an alternate media and stored securely offsite in accordance with the KRS Business Continuity/Disaster Recovery Planning Policy.

6. Service/maintenance vendors shall be required to sign a KRS Confidentiality Agreement in accordance with the KRS Conflict of Interest and Confidentiality Policy prior to service/maintenance of KRS equipment. Service and maintenance shall be performed onsite where practicable. In the event the equipment must be removed temporarily from KRS premises for service, all sensitive data shall be securely removed from the equipment in accordance with the KRS Computer Sanitization Policy.

7. KRS shall develop and implement procedures for performing periodic vulnerability assessments of KRS business resources.

Section 6: Data Sharing

1. All employers, contractors, vendors, suppliers, etc., that request limited access to data shall agree to comply with requirements as outlined in the KRS Confidentiality Agreement.

2. All employers, contractors, vendors, suppliers, etc. shall be prohibited from transferring KRS data to other third-party entities unless authorized by KRS.

3. All data shared with external entities shall have personal identifiers removed unless their use is necessary for conducting KRS business.

4. Data classified for public access shall be made available upon request in accordance with the Kentucky Open Records Act (KRS 61.870-844).

5. Sensitive KRS data shall not be provided over the telephone unless the identity of the individual can be confirmed (i.e. use of PIN).

Section 7: Data Disclosure

1. All incidents of data disclosure shall be reported to the employee’s manager and the KRS ISO in accordance with the KRS Security Incident Reporting and Handling Policy.

2. KRS shall assess the likely risk of harm caused by a disclosure and notify its members in accordance with the KRS Disclosure Policy.